Community

Follow

Like

Blog Post

Login

RSS Feed

Technical Articles

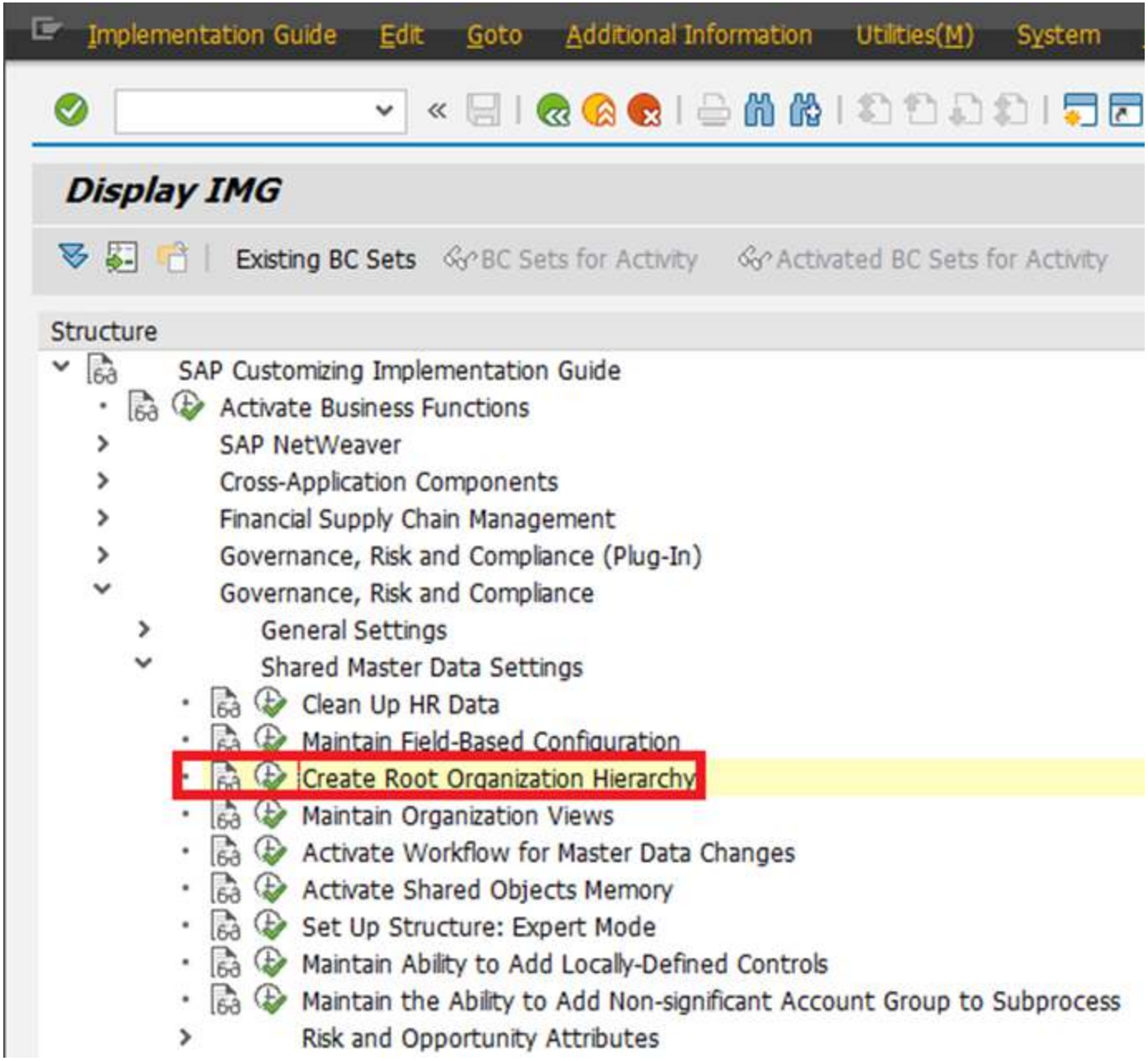
Madhu Babu #MJ

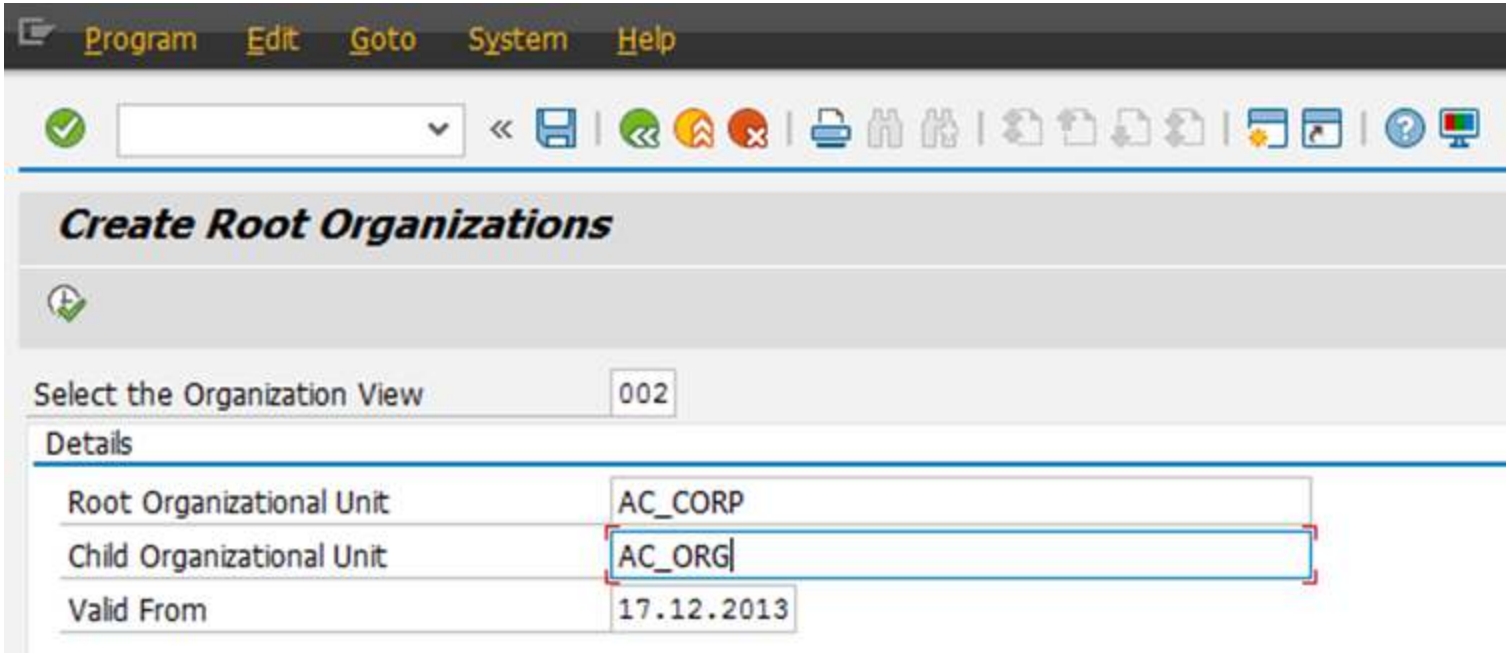
January 17, 2014 | 4 minute read

SAP GRC 10.0/10.1/12.0 – Creation of Mitigation Controls

29 28 56,269

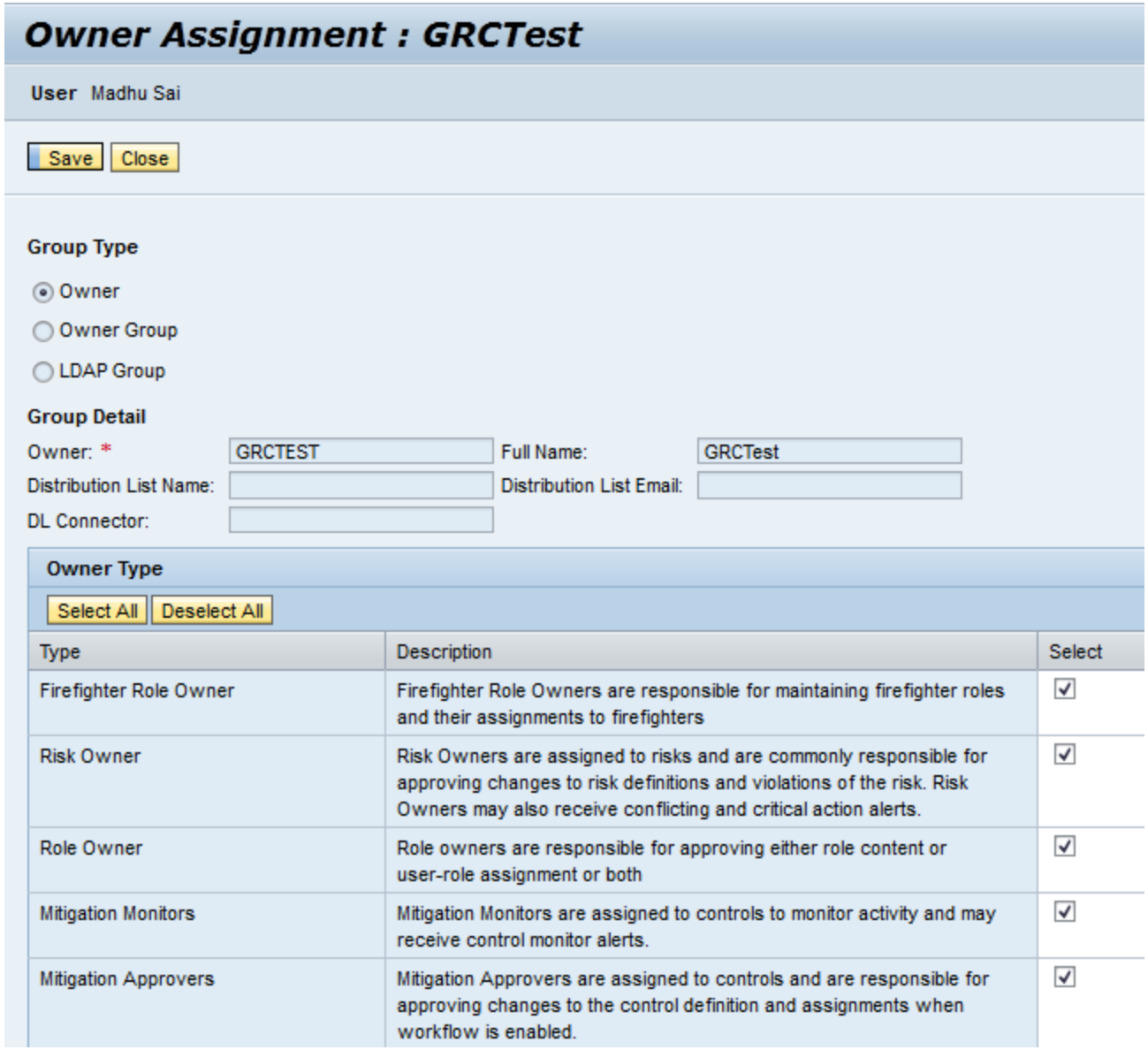
1. Before creating mitigating controls you need to create a Root Org entry, this replaces the Business Units in previous AC versions. Navigate to the IMG under Shared Master Data Settings and create a Root Org as shown below:


Implementation Guide
Edit
Goto
Additional Information
Utilities(M)
System
Display IMG
Existing BC Sets
BC Sets for Activity
Activated BC Sets for Activity
Structure
SAP Customizing Implementation Guide
Activate Business Functions
SAP NetWeaver
Cross-Application Components
Financial Supply Chain Management
Governance, Risk and Compliance (Plug-In)
Governance, Risk and Compliance
General Settings
Shared Master Data Settings
Clean Up HR Data
Maintain Field-Based Configuration
Create Root Organization Hierarchy
Maintain Organization Views
Activate Workflow for Master Data Changes
Activate Shared Objects Memory
Set Up Structure: Expert Mode
Maintain Ability to Add Locally-Defined Controls
Maintain the Ability to Add Non-significant Account Group to Subprocess
Risk and Opportunity Attributes



2. You will need to:

- Create User in SU01 master in GRC.
- Run the user sync jobs in GRC.
- NWBC – Access Management – Access Control Owners – Create an entry and select owner type as Mitigation Monitor or Mitigation Approver

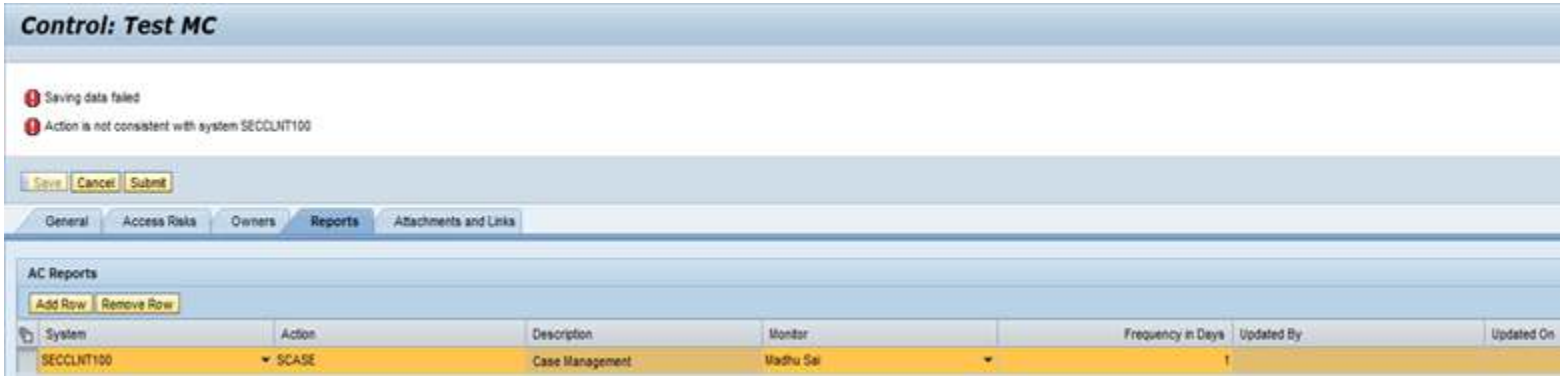

Owner Assignment : GRCTest
User Madhu Sai
Save
Close
Group Type
Owner
Owner Group
LDAP Group
Group Detail
Owner: *
GRCTEST
Full Name:
GRCTest
Distribution List Name:
Distribution List Email:
DL Connector:
Owner Type
Select All
Deselect All
Type
Description
Select
Firefighter Role Owner
Firefighter Role Owners are responsible for maintaining firefighter roles and their assignments to firefighters
Risk Owner
Risk Owners are assigned to risks and are commonly responsible for approving changes to risk definitions and violations of the risk. Risk Owners may also receive conflicting and critical action alerts.
Role Owner
Role owners are responsible for approving either role content or user-role assignment or both
Mitigation Monitors
Mitigation Monitors are assigned to controls to monitor activity and may receive control monitor alerts.
Mitigation Approvers
Mitigation Approvers are assigned to controls and are responsible for approving changes to the control definition and assignments when workflow is enabled.

- NWBC- Master Data – Organization – Assign user in Owner tab. After assigning the user to the organization then user can be maintained as Mitigation Approver/Monitor during Mitigation Control creation workflow.

Organizations
View: Standard Hierarchy
Date 17.12.2013 Apply Advanced Open Add Remove Actions
Name
Organization Hierarchy
AC_CORP
AC_ORG
Details
Name: AC_CORP
Organization
Organization: AC_CORP
Parent Organization - ID 50000001
Timeframe 17.12.2013 Effective Date 17.12.2013
Save Cancel
General Subprocess Indirect Entity-Level Controls Regulations Policies Objectives Key Risk Indicators Units of Measure Risk Appetite Risk Thresholds Users Owners
AC Owners
Add Row Remove Row
Name Type User ID Updated By Updated On
Madhu Sai Owner MSAI MSAI 17.12.2013
GRCTest Owner GRCTEST MSAI 17.12.2013

3. Now create mitigation control from NWBC -> Setup -> Mitigation Controls -> Create

In SP13, when we are adding actions in the reports tab, an error message pop-up as shown below.



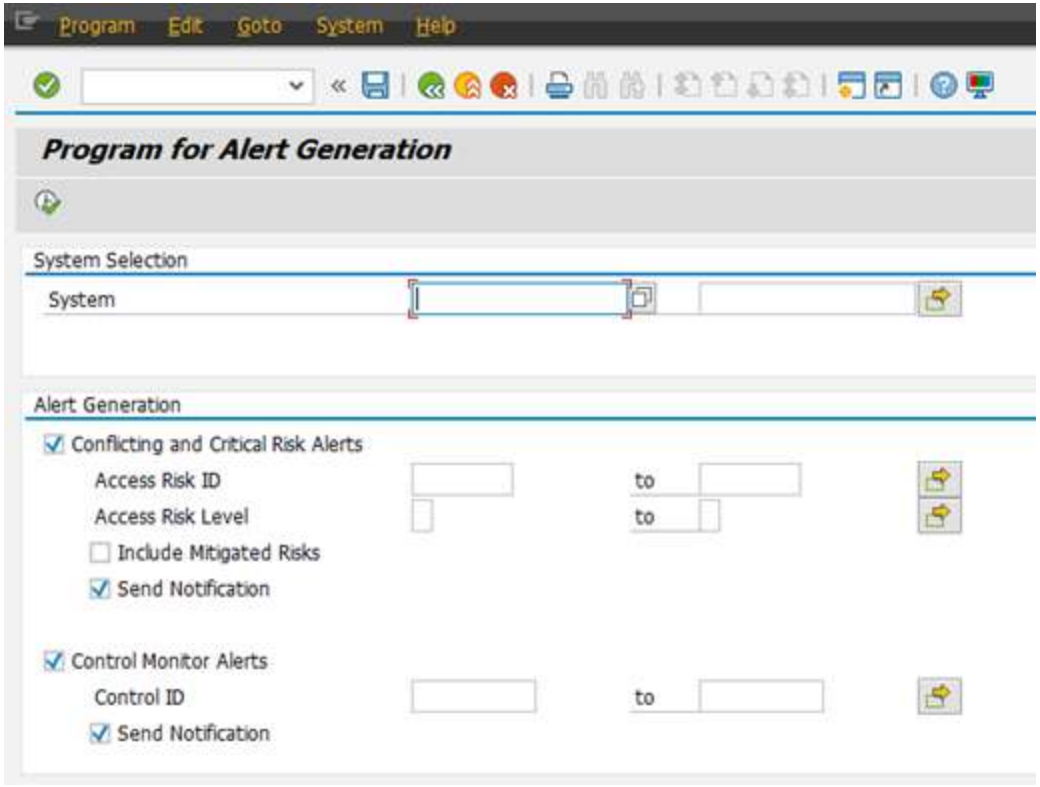
Saving data failed

Action is not consistent with system SECCLNT100

Without the report the mitigation saves without issue. I am also adding the Action value by clicking F4, searching and then adding it. To resolve this implement SAP Note: 1902129 – Unable to save Mitigation control after adding AC Report

Mitigation Monitor: Mitigation monitor is the one who would be checking whether mitigation is being performed. This monitoring can be done either manually or alerts can be sent to the monitor. “Reports” which are maintained in reports tab of mitigating control, will trigger an e-mail to the Mitigation approver if control monitor does not run that report with in the frequency mentioned.

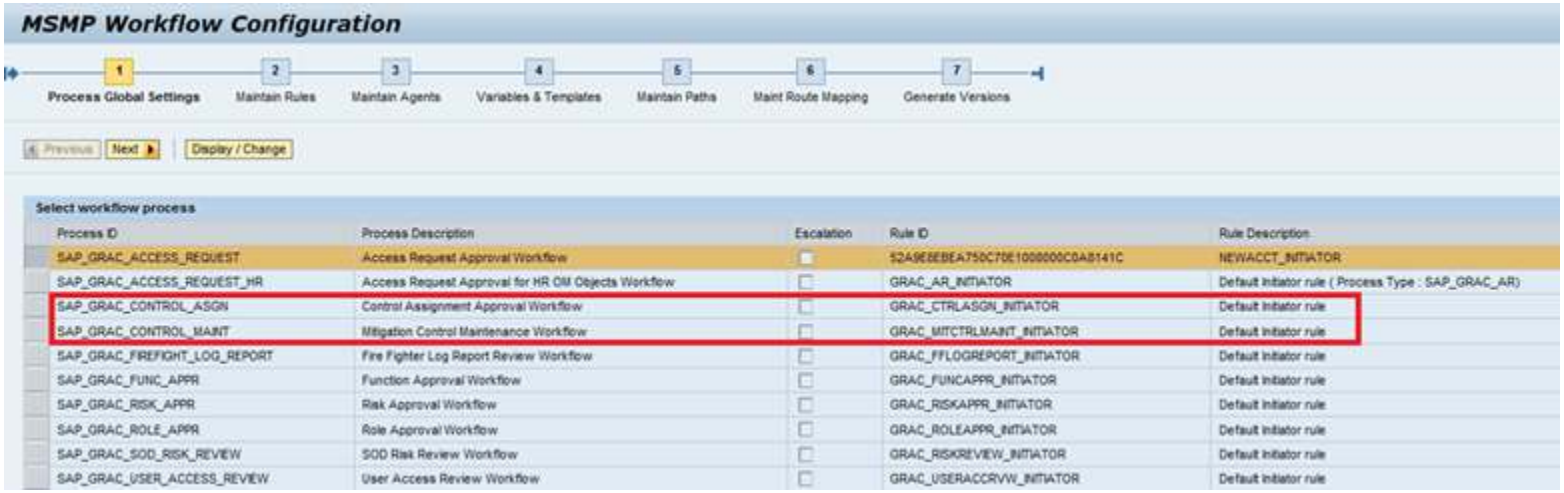
Alerts can be set through the program mentioned below by executing the Tcode **GRAC_ALERT_GENERATE.**



-

Mitigation Approver: Mitigation Approvers are assigned to controls and are responsible for approving changes to the control definition and assignments when workflow is enabled. In GRC 10.0 we have predefined workflow for this. We need to maintain the below configuration settings in SPRO.

Below mentioned standard workflows needs to be enabled.



Issues with Deletion of Mitigation Controls or MC assignments:

When deleting Mitigation Controls or Mitigation control assignments, we used to a get a message task executed but deletion was not happening. After implementing the steps mentioned below issue was resolved.

1.Run transaction SM30

2. Display the view GRFNPARENT in change mode

3. Add new line

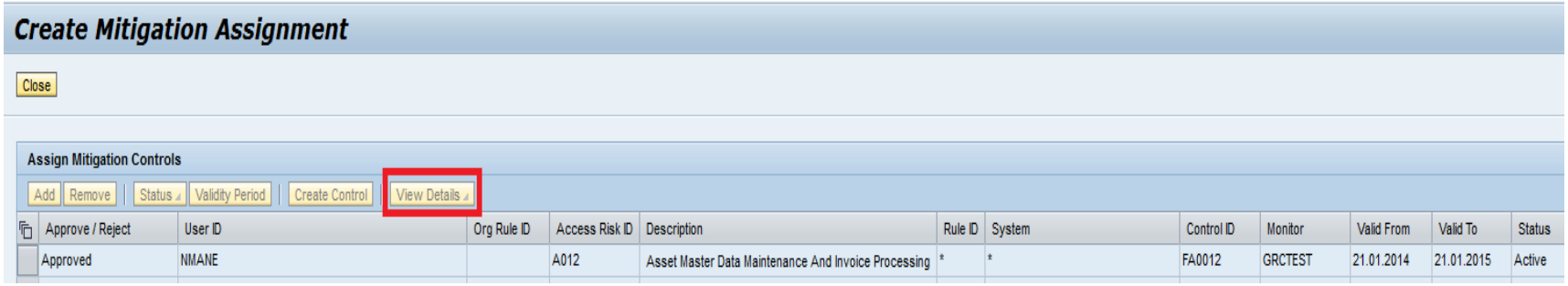
4. Entity = SUBPROCESS

5. Parent = ORGUNIT

Mitigation Control Assignment Workflow

-

In GRC we have standard SAP provided workflow for Mitigation control assignment. I have come across few queries w.r.t this workflow as the mitigation assignment approver is not able to view the details as the “VIEW DETAILS” button is greyed out as shown in below screen.



Transport Organizational Units & Mitigation Controls

There is no Transport Mechanism to move the Business Units/Organizational Units & Mitigation Controls from one Landscape to another Landscape in GRC Suite, because it is Master Data.

There is no Download & Upload functionality available for these Controls to move from one Landscape to another. Organizational Units & Mitigation Controls are tied together as these are shared among GRC Access Controls & Process Controls.

You need to recreate it in Destination Environment as Transport/Movement is not possible.

When you create the Organizational Unit with the Description in GRC, the System will generate a unique number for Organization Unit, which will be different for each system. That was the reason, we need to recreate Organizational Unit in each System.

But, Mitigating Control Assignments of User/Role/Profile/User Org/Role Org can downloaded from

one Landscape & can upload it to another Landscape.

Most convenient way to change existing mitigations is to use standard ABAP program for download and upload.

Go to SA38 and use the following programs:

GRAC_UPLOAD_MIT_ASSIGNMENTS

GRAC_DOWNLOAD_MIT_ASSIGNMENTS

Once you have downloaded the full list into an Excel file you can do your adjustments and upload it again. Hope this would be helpful.

For understanding the Mitigation control life cycle, please go through the below blog by Alessandro for basic and process oriented understanding for Mitigation control Lifecycle

-

Mitigating Control Lifecycle

Alert Moderator

Assigned Tags

SAP Access Control | SAP GRC Access Enforcer for SAP NetWeaver | governance risk and compliance sap grc | grc 10.0 | mitigation | mitigation controls

Similar Blog Posts

SAP Access Control - Useful Documents, Blogs, Resources, etc.

By Alessandro Banzer Aug 19, 2014

SAP GRC Access Control 10.0/10.1/12.0 - De-Centralized EAM

By Madhu Babu #MJ Jan 16, 2014

SAP GRC 10.0/10.1/12.0 - Mitigation Policy Configuration for Access Requests

By Madhu Babu #MJ Jul 08, 2016

Related Questions

Is it possible to access and approve GRC request through mobile app ?

By Pranjal Garg Dec 14, 2020

can we upload rule sets from GRC 0.0 to 10,1

By Former Member Jan 20, 2018

Integration of GRC AC 12 with HR Trigger

By Bruno Marcio Neto de Oliveira Jul 10, 2020

29 Comments

You must be Logged on to comment or reply to a post.

Former Member
January 17, 2014 at 4:42 am

hi Madhu,

thanks for sharing your view and its been very useful. But I got a doubt why the business process has been replaced by ORG unit if both serves the same purpose?

regards,

dhanunjay

Like 0 | Share

Madhu Babu #MJ | Blog Post Author
January 17, 2014 at 5:29 am

Hi Dhanu,

Thanks for taking your time in going through the document.

Its not business process. It is business unit in GRC 5.3 and now it has been changed as Organization. The main purpose of doing this is to allow sharing of mitigation controls between AC and PC using common org.hierarchy. Users can also maintain different views of org.structures depending on their needs which was missing with business unit concept.

Regards,

Madhu.

Like 0 | Share

Former Member
January 17, 2014 at 5:48 am

Hi madhu,

Thanks for clarifying this.

looking for more inputs from you in the future.

regards,

dhanunjay

Like 0 | Share

Suvonkar Bashak

January 21, 2014 at 12:19 pm

Hi Madhu,

Nice effort on the walkthrough over the mitigation control creation.

Regards,

Suvonkar

Like 0 | Share

Faisal Khan
January 27, 2014 at 6:09 am

Madhu,

Good efforts and seems you have documented all the details!

Regards,

Faisal

Like 0 | Share

Madhu Babu #MJ | Blog Post Author
January 27, 2014 at 9:05 am

Thanks Faisal. I am still updating it with any queries i come across so that it can be one stop for the people looking for help regarding Mitigation Controls in GRC 10.

Like 0 | Share

Nguyen Huynh
February 5, 2014 at 8:38 am

Nice document. Thanks.

Have you face a strange behavior of control change? Once a control is assigned to user, changing the monitor is more possible. Could you solve this problem?

Like 0 | Share

Former Member

February 28, 2014 at 1:15 pm

Nice Document and lot of important details mentioned in the document. Very good effort.

Thanks,

Prasad

Like 0 | Share

Rudolf Staudacher

March 2, 2014 at 10:02 am

very helpful document and good overview for migitation creation with prerequisites.

addtional helpful woud be:

a) Link to basic/official Mitigation Help

b) Test description

Thanks
Rudi

Like 0 | Share

Arif Mahamud

March 2, 2014 at 1:32 pm

good really helpful

Like 0 | Share

Madhu Babu #MJ | Blog Post Author

March 3, 2014 at 8:42 am

Hi Rudolf,

Thanks a lot for your feedback. I have recently come across a blog which helps you with basic mitigation understanding.

Mitigating Control Lifecycle

b. Test description ? I cannot understand about this. Can you be specific? If you want me to explain any example scenario from business point of view?

Regards,

Madhu.

Like 0 | Share

Madhu Babu #MJ | Blog Post Author

March 3, 2014 at 8:43 am

Thanks all for your feedback. If you have any points which adds more value to this blog, please suggest.

Regards,

Madhu.

Like 0 | Share

Rudolf Staudacher

March 3, 2014 at 9:58 am

Hi Madhu,

another finding was helpful for me:

... Access Risk Mgmt-Guide http://scn.sap.com/docs/DOC-1573

Like 0 | Share

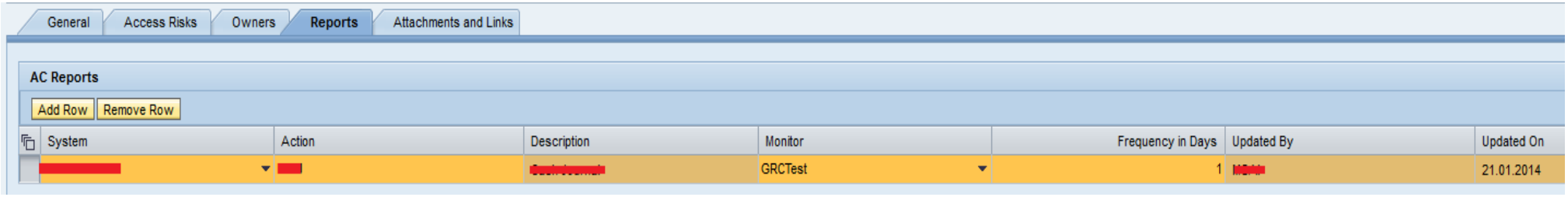
Madhu Babu #MJ | Blog Post Author

April 16, 2014 at 9:34 am

Hi Neeraj,

Under Reports tab i don't think you will have any other tabs.

Reports Tab Details



Access Controls is used as a documental tool for Mitigating Controls, rather than a implementing tool, i.e. you apply the control against the role/user, but the actual application of the control is performed outside of Access Control. This may be realized by running a custom SAP report to monitor the usage of the risky functions within the ECC system etc.

Action is for the t-code of the SAP Report. A brief explanation below will help in understanding

If you have a mitigation control that Mr. Z will run X report using Y t-code on a frequent basis of monthly or quarterly and reviews the report.

Then you need to give that Report name- X, in Action - Y T-code and frequency as Monthly/Quarterly. This helps for the system to check if the t-code has been executed or not in that frequency by the Monitor and generates a Alert [based on alert generation configuration]. If the monitor doesn't execute the action in backend in the set frequency, we will find an alert in Alert monitor- control monitoring, but if the monitor executes the action we will NOT get alert.

The role of Monitor is to see whether everything that was risky from the access being mitigated is fine or not. That is, he/she would see to it that the user who has been given extra excess or conflicting access has not misused it. Every Mitigation control, for this purpose has a Monitor attached to it who does this job

Action - This is some tcode a monitor has to execute in backend to see that reports.

A. E.g. if someone is doing check payment entry(risk), and mitigation is done for a user/role, there must be a tcode where we can check what payments are made(sorry I am not well versed in FI Tcodes) , this tcode will be put in action tab and monitor will have to check it via that particular tcode.

Frequency is simply what the period you want to set within which a monitor must perform this activity - say one week or one month.
If a monitor doesn't execute that action/tcode within that time, an alert will be generated and mail will be triggered to mitigation approver (indicating that supposed task is not being performed).

Mitigating alerts check if a mitigation alert monitor has actually run the report that has been assigned in the control, in the defined period. He needs to have run that report at least once in order for this to work (so that CC can calculate the control period).

Regards,
Madhu.

Like 0 | Share

Madhu Babu #MJ | Blog Post Author
April 16, 2014 at 3:39 pm

Hi Neeraj,

This issue looks weird. Can you provide your GRC SP details?

Regards,

Madhu.

Like 0 | Share

Neeraj Agarwal

April 17, 2014 at 2:45 am

We are on SP14.

Like 0 | Share

Former Member

April 18, 2014 at 6:35 am

Hi Neeraj,

Modify the application in admin mode and modify the display. It will solve your provblem.

BR,

Mangesh

Like 0 | Share

Faisal Khan

June 16, 2014 at 3:23 pm

Hi Madhu,

Thanks for your document!

It is really very good . Your efforts are appreciated.

Can you help me with below?

I defined the mitigation controls with owners and monitors. Frequency is also maintained in them.

I scheduled GRAC_ALERT_GENERATE this program in background on daily basis. My understanding was that, Control Monitor would receive email notifications if he fails to execute the reports/transaction codes in the target system.

What is happening is that, daily on scheduled time, Control Owner is receiving email notifications with details of the control and their respective monitors. However, Control Monitors are not getting the email notifications!

What do you think I missed?

Proper email ids are maintained for all monitors in SU01 and email server is configured. Other ARQ email notification are duly sent.

Do I have to run any other job for sending email notifications to control monitors?

Can you advise?

Regards,

Faisal

Like 0 | Share

Kesava Mullati

September 3, 2014 at 9:58 am

Hi Madhu,

Thank you for the document. I have a one remark on Reports tab.

As per the document:

"Reports" which are maintained in reports tab of mitigating control, will trigger an e-mail to the Mitigation approver if control monitor does not run that report with in the frequency mentioned.

My Query:

Can GRC AC has the functionality to check the back-end system whether control monitor execute the report or not with in the maintained frequency. I think this functionality is available in PC. Could you please clarify me on this part?

Thanks in advance

Regards,

Kesava

Like 0 | Share

Khaleel Syed

December 10, 2014 at 2:56 am

Hi Madhu

I created root entry , created a users in grc system with profile sap_all,Created an entry and selected owner type as Mitigation Monitor or Mitigation Approver in NWBC,

while trying to assign user in owner tab in org , iam not able to find the those users in the search list..

please suggest

Like 0 | Share

Madhu Babu #MJ | Blog Post Author

December 11, 2014 at 1:53 am

Hi Khaleel,

Please assign Control Approver and Control Monitor roles to your Users and test it. I assume SAP_ALL will not have GRC related authorization objects.

SAP_GRAC_CONTROL_APPROVER

SAP_GRAC_CONTROL_MONITOR

Regards,

Madhu.

Like 0 | Share

Former Member
December 4, 2015 at 11:11 pm

Hi Madhu,

Thanks for this!

I'm good with the above steps up until the last bullet point in step 2. You say, "Assign user in Owners tab...". I've tried this now multiple times in a variety of different ways, and it's not working.

Essentially what happens is that I navigate to the Owners tab, add a row, input the name of a user that has already been defined as an owner, and click Save. The Organization window closes and a message appears at the top of the Organization Hierarchy window, "Organization updated successfully." However, when I open the organization up again, the user that I just entered and saved isn't there. No matter what I do, I can't get the system to actually save a user in the Owners tab!

Any ideas about what I'm doing wrong??

Thanks so much in advance!!

Amanda

Like 0 | Share

Ilona Krawiec

September 24, 2020 at 10:31 am

I would also like the answer to that. What is the "Users" tab for. If I have someone there, then I cannot assign this user in the "Owners" tab. Who knows what the tab Users does?

Thanks so much in advance!

Like 0 | Share

Pranjal Garg

December 29, 2015 at 7:54 am

Hi All,

Nice document it is, but my problem is that my mitigations is coming in non alphabetic order, when user is trying to mitigate the user so the list opens in LOV is in non alphabetic order, is their a way to change this settings so that monitor comes in right way

Like 0 | Share

Pranjal Garg

March 6, 2016 at 7:34 pm

Do we have a way here to restrict that monitor cant be able to assign itself as a monitor.

Like 0 | Share

Kent Myska

April 15, 2016 at 8:56 pm

Hi All,

I am having trouble getting the Mitigating Monitors to appear in the right order when mitigating. We migrated from 5.3 and now in 10.1 when I add new Monitor in the Access Control Owners window it appears in alpha order by Owner ID, but when in the Organizations window (where I assigned the new monitor to the org hierarchy), he is appearing at the bottom of the list, but should not be. Also where I assign the Monitor to a Control he appears last. Hence the result is that when one goes to mitigate and assign a monitor, the list on Monitors to choose from is not in true alpha order.

Thanks

Kent

Like 0 | Share

sirisha vuyyuri
July 4, 2016 at 1:44 pm

Awesome Document.!!

Like 0 | Share

Manoj Varma
May 3, 2021 at 10:38 am

Hi Madhu,

i am unable to delete the Root Org in GRC Dev system. Could you please help.

Thank you

Manoj

Like 0 | Share

GURUGOBINDA HARICHANDAN PARIDA
October 11, 2021 at 11:14 am

Hi Manoj,

Hope your query has been resolved - "i am unable to delete the Root Org in GRC Dev system. Could you please help.".

Best Regards,

Guru

Like 0 | Share

Find us on

Privacy	Terms of Use
Legal Disclosure	Copyright
Trademark	Cookie Preferences
Newsletter	Support